

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
STATESVILLE DIVISION
CRIMINAL ACTION NO. 5:21-CR-00043-KDB-DCK**

UNITED STATES OF AMERICA,

Plaintiff,

v.

MICHAEL DALE BONDS,

Defendant.

ORDER

THIS MATTER is before the Court on Defendant’s Motion to Suppress (“Motion”) (Doc. No. 14). For the reasons discussed below, the Court will **DENY** the Motion to Suppress.

I. RELEVANT BACKGROUND

On June 27, 2020, the National Center for Missing and Exploited Children (“NCMEC”) received a submission to its “CyberTipline” from Google (Doc. No. 15-2). The submission indicated the presence of “apparent child pornography” stored in the Google Drive infrastructure¹ associated with the user account “luvenit2222@gmail.com”. *Id.* Google provided NCMEC with subscriber information for the user as well as IP addresses. *Id.* The report listed seven files flagged by Google, along with an image categorization. *Id.* at 22. According to Google, six of the files depicted a pubescent minor engaged in a sex act.² *Id.* One of the files depicted a prepubescent

¹ The Google Drive is a cloud-based storage service where users can store, share, and collaborate on files and folders from their devices. *See* Google Drive, <https://www.google.com/drive/> (last accessed October 5, 2021).

² Google defined “sex act” as “any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.” (*See* Doc. No. 15-2, p. 22).

minor engaged in a sex act according to Google. *Id.* Google further reported that an employee had viewed the entire contents of one of the files, specifically “Google-CT-RPTd5935890081177a14ccf24ac61b5c35f-Copy of 756a3a3b-57cc-484e-9491a41d2d59b8f2.mp4”, concurrently or immediately preceding the sending of the CyberTipLine Report. *Id.* at 20. The other files were not reviewed, but a Google employee had previously reviewed a file with the same hash value³ and had already determined that it contained apparent child pornography. *Id.* at 4.

Based off the information provided by Google, on November 24, 2020, NCMEC sent the CyberTip to the North Carolina Internet Crimes Against Children Task Force. They assigned it to Detective Garron Lawing (“Det. Lawing”) with the Mooresville Police Department (“MPD”). Det. Lawing received a copy of the CyberTip from Google, labeled as CyberTipLine Report 74146734 (Doc. No. 15-2). On that day, Det. Lawing reviewed all the information provided by Google, including the files that allegedly contained child pornography. He then applied for a state search warrant for the Google account, luvenit2222@gmail.com. (*See* Doc. No. 15-3). The search warrant was issued and served on Google. However, prior to receiving any data from Google, Det. Lawing withdrew the search warrant. (*See* Doc. No. 15-4) (record showing status as withdrawn).

On December 14, 2020, Det. Lawing applied for another state search warrant for the information and files provided by Google (*See* Doc. No. 15-1). In the affidavit, Det. Lawing explained the information provided by Google. *Id.* The affidavit further described the process by

³ When a Google employee finds child pornography on its servers, it is given a “hash” and added to the database. A Google employee visually inspects and confirms an image to be apparent child pornography before it is added to the database. *United States v. Miller*, 982 F.3d 412 (6th Cir. 2020). If the hash value of the file sent, received, or uploaded by a user matches the hash value of a file in its database of known child pornography, or if an employee reviews a file and sees child pornography; Google submits a report to the CyberTipLine that is operated by the NCMEC. *Id.*

which Google detected child pornography that was sent, received, or uploaded through its systems, including by monitoring hash values. *Id.* Det. Lawing included a description of the one file, Google-CT-RPTd5935890081177a14ccf24ac61b5c35f- Copy of 756a3a3b-57cc-484e-9491-a41d2d59b8f2.mp4, that was viewed by an employee at Google concurrent with the submission of the CyberTip. *Id.* The file depicted three boys, aged 10 to 12 years old, fully nude and performing oral sex on each other. The warrant was signed by a North Carolina Superior Court Judge and executed (Doc. No. 15-1). Pursuant to this search warrant, all seven of the files provided by Google could be examined. *Id.*

Next, on December 15, 2020, Det. Lawing sought a third state search warrant for the Google account, luvenit2222@gmail.com (*See* Doc. No. 15-5). In support of this search warrant, Det. Lawing discussed the search warrant he had previously obtained for the Cybertip and provided the names of files and a description of all seven videos. *Id.* The warrant was signed by a North Carolina Superior Court judge and executed. Google complied with the December 15th search warrant and provided Det. Lawing with data associated with the luvenit2222@gmail.com account on January 6, 2021.

Det. Lawing then used the information he gathered from the December 14th Cybertip search warrant and December 15th Google search warrant to apply for a final search warrant for the residence of the Defendant, 102 Daventry Place, Mooresville, North Carolina (*See* Doc. No. 15-6). The search warrant was executed on January 12, 2021. The detective located evidence of the luvenit2222@gmail.com account on devices in the home. Child pornography was located on a laptop. Defendant told the detective that someone had put child pornography in his account and that he tried to get rid of it by sending it to another email account.

Defendant filed his Motion to Suppress on August 31, 2021, moving this Court to exclude evidence obtained from the searches of his residence and private electronic data, the seizures of his electronic devices and digital media, and any statements obtained in connection with and resulting from the searches. Specifically, Defendant argues law enforcement violated his Fourth Amendment rights and that any evidence seized pursuant to the four search warrants should be suppressed because they rely on information obtained through a warrantless and unconstitutional search of the seven files from Defendant's Google Drive.

II. DISCUSSION

The Fourth Amendment of the United States Constitution guarantees “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures... and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. It is well-settled that Fourth Amendment protection extends to a person's electronically stored files, data, e-mail attachments, and the like. *See Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967)). Fundamental to the Fourth amendment is that it protects the rights of the people against conduct by the *government*, not private individuals. *See United States v. Richardson*, 607 F.3d 357, 364 (4th Cir. 2010).

A. The Private Search Doctrine

The “private search” doctrine is implicated when a private party conducts a search of private information and the government subsequently reviews that same information without first obtaining a search warrant. *United States v. Fall*, 955 F.3d 363, 370 (4th Cir. 2020). The “private search” doctrine's foundation is built on the rule that one can only invoke the Fourth Amendment's protection where he has a legitimate expectation of privacy. *Rakas v. Illinois*, 439 U.S. 128, 143

(1978); *see also Oliver v. United States*, 466 U.S. 170, 177 (1984) (A legitimate expectation of privacy is both subjective and objective in nature. A defendant must show that he had a subjective expectation of privacy; and the expectation is one that society recognizes as reasonable). However, once invoked, an individual's expectation of privacy does not last indefinitely. An expectation of privacy can be "frustrated", or in other words, it can be eliminated. In this circumstance, the Fourth Amendment no longer offers protection from governmental intrusion. The most common example of when an expectation of privacy is frustrated is when information is revealed to a third party. *United States v. Jacobsen*, 466 U.S. 109, 117 (1984) ("[i]t is well-settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information."). The "private search" doctrine consequently allows the government to search where an individual's expectation of privacy has already been frustrated by an initial private search without implicating the Fourth Amendment.

The Supreme Court's decision in *United States v. Jacobsen* best articulates the "private search" doctrine in practice. In *Jacobsen*, FedEx employees found what they believed to be illegal drugs in a damaged box after they had opened it. *Id.* at 111. The United States Drug Enforcement Administration ("DEA") was notified by FedEx and the drugs were placed back in the box until their arrival. *Id.* When the DEA arrived, they replicated the search previously performed by the FedEx employees. *Id.* at 111-112. The Supreme Court held that the Fourth Amendment is not implicated when a private entity acts in a private capacity and that a private search frustrates an expectation of privacy. *Id.* at 117. Thus, law enforcement does not violate the Fourth Amendment

when they simply replicate the initial private search. *Id.* (“[t]he Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated”); *United States v. Fall*, 955 F.3d at 370; *United States v. Runyan*, 275 F.3d 449, 461 (5th Cir. 2001) (Under the private search doctrine, “the critical inquiry under the Fourth Amendment is whether the authorities obtained information with respect to which the defendant’s expectation of privacy has not already been frustrated”); *see also Coolidge v. New Hampshire*, 403 U.S. 443, 489 (1971) (The police need not “avert their eyes” when presented with evidence obtained in a private search).

In *Jacobsen*, the Fourth Amendment was not implicated because the DEA’s search of the box allowed the agents to learn “nothing that had not previously been learned during the private search.” *Id.* at 120. This established that under the “private search” doctrine invasions of privacy by the government must be tested by the degree they exceed or expand the initial private search. *Id.* at 115; *see also United States v. Fall*, 955 F.3d at 370. Therefore, to determine whether the “private search” doctrine is appropriate in this case, the controlling question the Court must answer is whether Det. Lawing exceeded the private search conducted by Google. If he did, then the Defendant’s rights under the Fourth Amendment were violated.

The Defendant analogizes this case to *United States v. Wilson*, No. 18-50440, 2021 U.S. App. LEXIS 28569 (9th Cir. Sep. 21, 2021). In *Wilson*, the Ninth Circuit held the Fourth Amendment was violated when the government conducted a search of files and that search was based on nothing more than the fact the hash values of the files matched the hash values of known child pornography. *Id.* at 44. However, even accepting the non-controlling authority of *Wilson*, the analogy is inapt because there is a crucial distinction between *Wilson* and the case before the Court. In *Wilson*, the internet service provider *did not* view any of the files before law enforcement did.

Id. at 29. The Ninth Circuit stated “the critical fact is that no Google employee viewed Wilson's files before Agent Thompson did. When the government views anything other than the specific materials that a private party saw during the course of a private search, the government search exceeds the scope of the private search.” *Id.* at 31. In this case, while Google flagged seven files on the Defendant’s account that they believed to contain child pornography, the warrant at issue relied *solely* on the one file that had been visually inspected by a Google employee (Doc. No 15-1).⁴ Although Det. Lawing had previously submitted a search warrant based on a description of all seven files (Doc. No. 15-3), importantly that search warrant was withdrawn before any evidence was provided by Google.⁵ Accordingly, while the Ninth Circuit held that searching files based only on hash value matches violated the Fourth Amendment, this Court need not and does not address that question here because those are not the facts of this case. Therefore, the analogy to *United States v. Wilson* is inappropriate.⁶

As discussed above, under the “private search” doctrine the key inquiry is whether the government expanded or exceeded the search conducted by the private party. *United States v. Jacobsen*, 466 U.S. at 115; *see also United States v. Reddick*, 900 F.3d 636, 638 (5th Cir. 2018) (quoting *United States v. Runyan*, 275 F.3d 449, 461 (5th Cir. 2001). In this case the Court need

⁴ The warrant also defined and described what a hash value is but provided no information on the content of the other files. *See* Doc. No 15-1.

⁵ No evidence was provided pursuant to this warrant so it cannot be the basis for a motion to suppress; there is nothing to suppress.

⁶ The Fourth Circuit has not yet considered that question, but other Circuits have held the Fourth Amendment does not prohibit an officer from opening and reviewing files after a private party has already determined that the files’ hash values matched known child-pornography images in its database. *See United States v. Miller*, 982 F.3d 412, 419 (6th Cir. 2020) (holding hash value matching does not implicate the Fourth Amendment pursuant to the private search doctrine), and *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018) (holding that any expectation of privacy was frustrated when a file’s hash value was compared against an existing database of known child pornography hash values).

only decide whether the viewing of the one file that was the basis for the December 14, 2020 warrant exceeded the initial private search. The Defendant argues that viewing the file allowed Det. Lawing to learn new information and therefore exceeded the initial private search, analogizing this case to *Walter v. United States*, 447 U.S. 649 (1980). However, this comparison also fails. In *Walter*, packages containing boxes of films were delivered to the wrong company and the company's employees opened the packages. *Id.* at 651- 652. The employees discovered that the boxes had "explicit descriptions" that suggested the films were possibly obscene. *Id.* at 652. The employees called the FBI and agents watched the films to confirm that they constituted obscenity. *Id.* The Supreme Court found a Fourth Amendment violation from the decision to watch the films without obtaining a warrant. *See Jacobsen*, 466 U.S. at 115-16 (quoting *Walter*, 447 U.S. at 657). Since private employees had seen only the labels, watching the films was a "significant expansion" of that search. *Id.* at 657. In this case, the Google employee viewed the *entire* file as opposed to just a description or a label (Doc. No. 15-2). The CyberReport stated the entire file had been viewed and described it.⁷ Therefore, Det. Lawing could not have exceeded the private search or committed an additional intrusion on the Defendant's privacy interest in the file because his expectation of privacy had already been frustrated as to the *entire* file. As a result, Det. Lawing did not obtain information that "had not previously been learned during the private search" by viewing the file.

The Defendant also questions the reliability of the Google employee, who remains anonymous. In both *Jacobsen* and *Walter*, law enforcement had direct, face-to-face contact with the private parties who initially conducted the searches and frustrated the expectation of privacy. The Defendant argues that this lack of face-to-face corroboration meant law enforcement was

⁷ Google's report categorized the file as a "B1" file. The definition of a "B1" file is one that contains images of a pubescent minor performing a sex act.

unable to contemporaneously verify the reliability of the information prior to conducting its search. The Court finds this argument unpersuasive. The Fourth Circuit has upheld convictions in cases where evidence was seized by an anonymous hacker and then provided to law enforcement. *See United States v. Jarrett*, 338 F.3d 339 (4th Cir. 2003) (also involving child pornography). Google is certainly not an anonymous hacker. Corporations like Google have specially trained individuals, who routinely create and submit these reports in the normal course of business. Google submitted 546,704 “CyberTips” in 2020 alone. NCMEC 2020 Reports by Electronic Service Providers (ESP), <https://www.missingkids.org/content/dam/missingkids/gethelp/2020-reports-by-esp.pdf> (last visited October 12, 2021). Additionally, Google provides an email address as a point of contact, which allows law enforcement to follow up, if needed.

In sum, Det. Lawing’s viewing of file, Google-CT RPTd5935890081177a14ccf24ac61b5c35f-Copy of 756a3a3b-57cc-484e-9491a41d2d59b8f2.mp4, which was the basis for the December 14, 2020 search warrant falls under the “private search” doctrine. The file had previously been searched and viewed in its entirety by a Google employee. This frustrated any legitimate expectation of privacy the Defendant had in it, and Det. Lawing could not and did exceed the search or obtain information that had not previously been obtained during the private search. Thus, the motion to suppress will be denied.

B. Good Faith

In the alternative, the Court finds the motion should be denied because Det. Lawing acted in good faith. Under the good faith exception to the exclusionary rule, evidence obtained by an officer who acts in objectively reasonable reliance on a search warrant will not be suppressed, even if the warrant is later deemed invalid. *United States v. Thomas*, 908 F.3d 68, 72 (4th Cir. 2018) (citing *United States v. Leon*, 468 U.S. 897, 922, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (1984)).

Evidence obtained from an invalidated warrant “will be suppressed only if ‘the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause.’” *United States v. Fall*, 955 F.3d at 371 (citing *United States v. Lalor*, 996 F.2d 1578, 1583 (4th Cir. 1993)).

In determining whether to suppress the fruits of an unconstitutional search, the Court must undertake a “rigorous” cost-benefit analysis, weighing the “deterrence benefits of exclusion” against its “substantial social costs.” *Davis v. United States*, 564 U.S. 229, 237–38 (2011). Those costs include interfering with courts’ truth-seeking function, and more specifically, concealing “reliable, trustworthy evidence bearing on guilt or innocence” and, in some instances, “set[ting] the criminal loose in the community without punishment.” *Davis*, 564 U.S. at 237. Exclusion is a “bitter pill” swallowed only where it would result in a “substantial deterrent effect” that outweighs its resulting costs. *United States v. Leon*, 468 U.S. 897, 907 n.6, (1984).

The Court is persuaded there is no conduct in this case that needs to be deterred and the cost of suppression would be high for the following reasons. First, Det. Lawing withdrew the initial warrant and sought additional ones when it was brought to his attention there might be a Fourth Amendment violation. Multiple circuits have held that the search of all seven files would have been constitutional.⁸ However, Det. Lawing still withdrew the warrant out of an abundance of caution to comply with the Fourth Amendment and Fourth Circuit precedent. Second, he acted reasonably in relying on the reported information from Google. Google, as discussed above, is a reliable source of information and therefore it was reasonable for Det. Lawing to rely on it and believe the information Google provided constituted probable cause. Lastly, the cost of

⁸ See *United States v. Miller*, 982 F.3d 412, 419 (6th Cir. 2020); *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018).

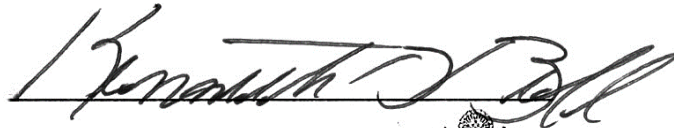
suppressing this evidence would be substantial. These files are reliable, trustworthy evidence bearing on guilt or innocence of the Defendant in this case and suppression of them would interfere with the truth-seeking function of this Court. Thus, suppression is not an appropriate remedy and the motion to suppress will be denied on the additional ground of Det. Lawing's good faith.

III. ORDER

IT IS THEREFORE ORDERED that Defendant's Motion to Suppress, (Doc. No. 14), is **DENIED.**

SO ORDERED.

Signed: October 13, 2021

A handwritten signature in black ink, appearing to read "Kenneth D. Bell", written over a horizontal line.

Kenneth D. Bell
United States District Judge

